AF/3621

PTO/SB/21 (08-03)
Approved for use through 08/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/589,747
Filing Date	9 June 2000
First Named Inventor	Neil Gilbert Siegel
Art Unit	3621
Examiner Name	Firmin Backer
Total Number of Pages in This Submission: 03	Attorney Docket Number: NG(MS)6336

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
- [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
- [ ] After Allowance communication to Technology Center (TC)
- [ ] Appeal Communication to Board of Appeals and Interferences
- [x] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Christopher P. Harris, Reg. No. 43,660 Tarolli, Sundheim, Covell & Tummino LLP
Signature	Christopher P. Harris
Date	February 18, 2004

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Lisa L. Pringle		
Signature	Lisa L. Pringle	Date	February 18, 2004

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 330.00

Complete if Known	
Application Number	09/589,747
Filing Date	9 June 2000
First Named Inventor	Neil Gilbert Siegel
Examiner Name	Firmin Backer
Art Unit	3621
Attorney Docket No.	NG(MS)6336

METHOD OF PAYMENT *(check all that apply)*

☑ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☐ Deposit Account:

Deposit Account Number

Deposit Account Name

The Director is authorized to: *(check all that apply)*

☐ Charge fee(s) indicated below ☐ Credit any overpayments

☐ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

	Extra Claims		Fee from below		Fee Paid
Total Claims		-20** =		X	=
Independent Claims		- 3** =		X	=
Multiple Dependent					=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	330.00
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 330.00

SUBMITTED BY				(Complete *(if applicable)*)	
Name (Print/Type)	Christopher P. Harris	*Registration No. (Attorney/Agent)*	43,660	*Telephone*	216.621.2234
Signature	Christopher P. Harris			*Date*	February 18, 2004

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

#15
3/3/04
mel

PATENT

CERTIFICATE OF MAILING

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date listed below.

Date: 02/18/2004

Lisa L. Pringle

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Neil Gilbert Siegel
Serial No.	:	09/589,747
Filing Date	:	June 9, 2000
For	:	SYSTEM AND METHOD FOR DISTRIBUTED NETWORK ACCESS AND CONTROL ENABLING HIGH AVAILABILITY, SECURITY AND SURVIVABILITY
Group Art Unit	:	3621
Examiner	:	Firmin Backer
Attorney Docket No.	:	199.38513X00
Confirmation No.	:	1612

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Following the Notice of Appeal filed on December 23, 2003, for the above-identified patent application, Appellants' Appeal Brief is hereby presented.

02/26/2004 JADD01 00000067 09589747
01 FC:1402 330.00 OP

1. REAL PARTY IN INTEREST

The real party in interest is Northrop Grumman Corporation.

2. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

3. STATU.S. OF CLAIMS

Claims 1-41 are pending. Claims 1-41 were finally rejected as being unpatentable over U.S. Patent No. 5,421,594 to Kung (Kung) in view of Matt Bishop, *Unix Security in a Supercomputing Environment*, IEEE Proceedings of the Supercomputing Conference, Reno, Nov. 13-17, 1989, New York, IEEE U.S., Vol. Conf. 2, November 13, 1989, pgs 693-698 (IEEE Supercomputing) in an Office Action dated August 26, 2003. Claims 1-41 are on appeal.

4. STATUS OF AMENDMENTS

No amendments have been filed subsequent to final rejection.

5. SUMMARY OF THE INVENTION

The present invention relates to a system and method for network access and control. FIG. 1 is an example of a wide area network 10 implemented in a military environment. The network 10 has military vehicles 30, each of which may contain at least one computer to access the network. In addition to military vehicles 30, at least one vehicle 40 is designated for a systems administrator or security officer (page 10, lines 14-18).

A local password file 1500 is installed on each computer in the network. The password file 1500 contains all user identifications and passwords for all authorized users of the network (page 10, lines 1-2). The password file 1500 can include the privileges associated with each user (page 13, lines 2-4) or the privileges can be contained in a separate file with pointers to the privileges stored in the password file (page 13, lines 7-9).

A user login module 1200 is provided for users to log in. The user login module displays a login screen to the user, one-way encrypts the password and determines if the local password file 500 contains a match (page 12, lines 9-11).

Each computer also has a channel monitoring and filtering module 1000. The channel monitoring and filtering module 1000 receives broadcast and multicast messages within the network 10 (page 12, lines 2-3). When a message is received, the channel monitoring and filtering module 1000 determines whether a currently logged in user has the security level or privileges to view the message (page 12, lines 4-5). If the user has the proper security level or privileges, the message is displayed (*Id.*).

A remote auditing module 1400 is provided in order to monitor and process anomalous or other security critical events (page 13 lines 10-13). These events include, but are not limited to when a user has exceeded the number of unsuccessful login attempts (page 13, lines 13-14), a message was rejected due to an invalid digital signature (*Id.* at line 20), a request for remotely loading passwords initiated by the systems security officer has completed successfully (page 14, lines 5-6), and/or when the local password file on a remote computer has been compromised (page 22, lines 4-6). When the remote auditing

module detects an anomalous event, the event is reported to the systems administrator or security officer (page 20, lines 7-8).

The systems administrator or security officer has several options available for responding to an anomalous event. The systems administrator or security officer can spoof the user into believing he has successfully logged into the system and wide area network (page 19, lines 18-19). The systems administrator or security officer can provide the user with false information intending to mislead the user (*Id.* at lines 19-21). Another option is to disable the computer and delete certain files on the disk drive or memory (page 19, 15-17, *cf.* page 20, lines 11-12). Yet another option available to the systems administrator or security officer is to lock the terminal screen and require the user to re-authenticate their user ID and password (page 19, lines 8-10). The re-authentication ID and password can be checked and confirmed by a master password file that is stored at the systems administrator's or security officer's computer system (page 14, lines 17-21).

A password management module 1300 is provided to enable updating of all local password files 1500 located within the wide area network 10 (page 112, lines 14-16). Each and every computer system in the wide area network including the systems administrator's or security officer's computer system contains an identical password file (*Id. at* lines 16-18). The system administrator's or security officer's password file is referred to as the master password file 1800 (*Id.* at lines 18-20). The system administrator or security officer (SA/SO) using a decrypted private key, digitally signs a message containing the master password file that is broadcast or multicast to all users or to targeted users on the network (page 16, lines 16-20). The recipients of the password file authenticate the digital signature using the

SA/SO public key which is stored locally on their systems (*Id.* at lines 20-22). If the digital signature has been authenticated, then the master password file is installed on the recipient's system as the local password file (page 17, lines 1-4). If the digital signature can not be authenticated, then the remote auditing module 1400 is executed (*Id.* at lines 8-12) and the event is reported to the systems administrator or security officer (page 20, lines 7-8).

6. ISSUES

I. Whether claims 1-41 are patentable under 35 USC §103 over Kung in view of IEEE Supercomputing.

7. GROUPING OF CLAIMS

It is believed that:

(1) Claims 1, 2, 4, 6, 8, 10-12, 20-24, 28, 31-35 and 39 stand or fall together.

(2) Claims 3 and 17 stand or fall together.

(3) Claim 5, 26 and 37 stand or fall together.

(4) Claims 7, 18, 25 and 36 stand or fall together.

(5) Claims 9, 27 and 38 stand or fall together.

(6) Claims 14, 29 and 40 stand or fall together.

(7) Claims 15, 30 and 41 stand or fall together.

It is believed that the claim groupings set forth above in (1), (2), (3), (4), (5), (6) and (7) do not stand or fall together. Reasons are set forth in the Argument Section 8 of this Brief.

8. ARGUMENT IN SUPPORT OF REVERSING THE FINAL REJECTION

A. AUTHORITY UNDER 35 USC §103

The MPEP sets forth the following criteria for an obviousness rejection under 35 USC §103:

> To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.
>
> *See,* MPEP §706.02(j).

For an obviousness rejection under 35 USC §103, the prior art must be analyzed at the time the invention was made. The use of the teachings of the present invention to find obviousness is impermissible.

> The court must be ever alert not to read obviousness into an invention on the basis of applicant's own statements; that is, we must view the prior art without reading into that art applicant's teachings. The issue, then, is whether the teachings of the prior art would, in and of themselves and without the benefits of appellant's disclosure, make the invention as a whole obvious.

In Re Sponnoble, 160 USPQ 237, 243 (CCPA 1969) (emphasis in original). Accordingly, the Examiner must consider only the teachings of the prior art references.

B. ARGUMENT IN SUPPORT OF REVERSING THE FINAL REJECTION OF CLAIMS 1-41

CLAIMS 1, 2, 4, 6, 8, 10-12, 20-24, 28, 31-35 AND 39

Independent claim 1 recites filtering and displaying messages to the user when a match is found on the one-way encrypted password file. Independent claims 20 and 31 recite a channel module and filter module to monitor and receive broadcast or multicast messages within the network and display the message to the user when the user's associated privileges permit viewing of the message.

Kung simply does not discuss filtering and displaying messages according to different level of user privileges contained within a one-way encrypted password file. The computer of any user attempting to log in will receive the same authentication message as that of any other user. Kung does not filter messages based on user permissions or privileges.

The aforementioned deficiency in Kung is not remedied by any teaching of IEEE Supercomputing. IEEE Supercomputing refers to access control mechanisms to regulate the ability to access resources such as files, devices and processes (page 695, col. 1, section 3 Access Control, Integrity and Least Privilege, paragraph 1). Each object is assigned a user and group identification (*Id.* at paragraph 2). Three sets of permissions are associated with each object, one corresponding to the user (owner), one to the group, and one to all others (*Id.*). When someone tries to access the object, the user permissions are checked, and if the user does not have permission then the group permissions are checked, otherwise the set of permissions for all others is checked (*Id.*). Thus, IEEE Supercomputing controls access to a resource, which is not the same as receiving and filtering messages

according to the user's permissions or privileges, nor does Kung teach or suggest a filter module to monitor and receive broadcast or multicast messages within the network and display the message to the user when the user's associated privileges permit viewing of the message as recited in the claims.

IEEE Supercomputing also teaches that no checking of any kind is performed to the privileged user root, also known as the supervisor, whereas the claims recite receiving and filtering messages according to user's permissions or privileges. Therefore, IEEE Supercomputing actually teaches away from what is recited in the claims.

Therefore, for the reasons set forth above, neither Kung nor IEEE Supercomputing, taken alone or in combination, teach or suggest filtering messages according to the user's permissions or privileges as recited in the claims. Therefore, the cited art does not teach or suggest all of the claim limitations. Accordingly, the rejection of claims 1, 2, 4, 6, 8, 10-12, 20-24, 28, 31-35 and 39 should be reversed.

CLAIMS 3 AND 17

Claim 3 recites notification to a systems administrator or security officer of the failure of a user to provide user identification and a one-way encrypted password that matches a user identification and a one-way encrypted password stored on the one-way encrypted password file. Claim 17, which depends from claim 16 recites reporting an anomalous event, *i.e.* when a user has exceeded the number of allowable unsuccessful login attempts, to a systems administrator or security officer.

The Kung reference does not discuss transmitting notification of failed log-in attempts to a system operator. The Office Action cites the user log-in rejection function within the

Kung system, where a failed log-on attempt causes the server to reject the log-in attempt and wait for another service request. It does not suggest, however, sending notification to a human operator of the failed log-in. The aforementioned deficiency in Kung is not remedied by any teaching of IEEE Supercomputing. Thus, neither reference teaches or suggests a notification to a system operator to report failed log-in attempts. Furthermore, neither system seeks human intervention.

Therefore, for the reasons set forth above, neither Kung nor IEEE Supercomputing, taken alone or in combination, teach or suggest notification to a systems administrator or security officer of the failure of the user to provide a user identification and a one-way encrypted password that matches a user identification and a one-way encrypted password stored on the one-way encrypted password file. Therefore, the cited art does not teach or suggest all of the claim limitations. Accordingly, the rejection of claims 3 and 17 should be reversed.

CLAIMS 5, 26 AND 37

Claim 5 recites spoofing the user into believing that access has been gained to the computer, the spoofing including the presentation of false messages and information to the user in response to a request by the systems administrator or security officer.

Claim 26 recites a remote control module to enable a systems administrator or security officer to spoof a user into believing that the access has been gained to a computer, the spoofing includes the presentation of false messages and information to the user. Claim 37 is for a remote control code segment to enable a systems administrator or security officer to spoof a user into believing that the access has been gained to a

computer, the spoofing includes the presentation of false messages and information to the user.

Neither Kung nor IEEE Supercomputing teach or suggest providing an unauthenticated user with false data in any form. The Office Action cites Kung (col. 4, line 60 – col. 5, line 18; FIG. 4, col. 5, lines 38-53 and col. 6, lines 18-50) for teaching spoofing a user into believing that the access has been gained to the computer, wherein the spoofing includes the presentation of false messages and information to the user. Applicant respectfully disagrees with the interpretation of these sections.

In rejecting claim 5, the Examiner (citing Kung col. 4, line 60 – col. 5, line 18) stated that Kung teaches a method further comprising spoofing, upon request by the systems administrator or security officer, the user into believing that access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user. However, Kung at col. 4, line 60 – col. 5, line 18 teaches that when a user logs into one computer of the distributed system, that when the user desires to use services at a second computer, the authentication information is forwarded to the second computer using a secure transport layer. This section does not teach spoofing a user into believing that the access has been gained to the computer, wherein the spoofing includes the presentation of false messages and information to the user.

In rejecting claims 26 and 37 the Examiner stated Kung (citing Fig. 4, column 5, lines 38-53 and column 6, lines 18-50) teaches a system wherein the appropriate action comprises spoofing, upon request by a systems administrator or security officer, the user into believing that access has been gained to the computer, wherein spoofing includes the

presentation of false messages and information to the user. However, Kung at column 5, lines 38-53 teaches that when a user enters user identification and a password it is compared against identification codes and encrypted passwords stored at the workstation. However, Kung at column 5, lines 38-53 does not teach does not teach spoofing a user into believing that the access has been gained to the computer, wherein the spoofing includes the presentation of false messages and information to the user.

Furthermore, Kung at col. 6, lines 18-50 teaches that a user logs into a workstation by providing user identification (ID) code and a password. After the user is logged in, when the user wants to access information stored in a remote computer, a secure communication procedure is requested to initiate a communication session with the remote computer. After a secure communication path 20a has been established, the user's ID code and encrypted password is transmitted to the remote computer. The user's ID and password are compared to a database coupled to the remote computer, and if they are the same, the user is permitted to log onto the remote computer. However, Kung at col. 6, lines 18-50 does not teach does not teach spoofing a user into believing that the access has been gained to the computer, wherein the spoofing includes the presentation of false messages and information to the user.

Therefore, for the reasons set forth above, neither Kung nor IEEE Supercomputing, taken alone or in combination, teach or suggest spoofing a user in response to a request by a systems administrator or security officer into believing that access has been gained to the computer, wherein the spoofing includes the presentation of false messages and

information to the user. Therefore, the cited art does not teach or suggest all of the claim limitations. Accordingly, the rejection of claims 3 and 17 should be reversed.

CLAIMS 7, 18, 25 AND 36

Claims 7 (claim 7 depending from claim 6) and 18 recite disabling a computer system and deleting a plurality of files from the computer system upon a request by the systems administrator or security officer. Claim 25, (claim 25 depending from claim 24, claim 24 depending from claim 20) recites a remote control module to enable a systems administrator or security officer to disable a computer and delete a plurality of files from the computer. Claim 36 recites a remote control code segment to enable a systems administrator or security officer to take action for an anomalous event by disabling the computer system so that the user cannot access the computer system and deleting a plurality of files stored in the computer.

Neither reference discusses remotely deleting system files to prevent an unauthorized user from accessing them. The portion of Kung cited in the Office Action describes communications between the host computer and the server, but does not discuss direct action by a systems administrator nor the deletion of system files for security purposes. Furthermore, neither reference discusses remotely disabling a computer and deleting files by the systems administrator or security officer.

Therefore, for the reasons set forth above, neither Kung nor IEEE Supercomputing, taken alone or in combination, teach or suggest disabling a computer system and deleting a plurality of files from the computer system upon a request by the systems administrator or

security officer. Therefore, the cited art does not teach or suggest all of the claim limitations. Accordingly, the rejection of claims 7, 18, 25 and 36 should be reversed.

CLAIMS 9, 27 AND 38

Claim 8 recites displaying a request for re-authentication at the direction of a system administrator or security officer. Claim 9, which depends from claim 8, requires that this re-authentication will take the form of a displayed log-in screen having a position for entry of the user identification and password. Claim 27 (claim 27 depending from claim 24, claim 24 depending from claim 20) recites a remote control module to enable a systems administrator or security officer to locking the computer and displaying a login screen for the user to re-authenticate the user identification and password in response to an anomalous event. Claim 38 recites a remote control code segment to enable a systems administrator or security officer to lock the computer and display a login screen for the user to re-authenticate the user identification and password.

In rejecting these claims, the Office Action cites Kung (Figs. 2, 3 and 4, column 5, line 54 - column 6, line 38, and column 4, lines 30-48) for describing an initial log-in procedure in rejecting these claims. However, these claims recite re-authentication, requiring an already authenticated user to re-enter a user identification and password upon the request of a system administrator. Neither Kung nor IEEE Supercomputing teach or suggest a re-authentication process.

Furthermore, the stated purpose of the Kung system was to avoid forcing a user to undergo the authentication process each time the user logged into a new remote host. (column 2, lines 56-60). The claims recite re-authenticating a user just to maintain the

present connection. Forcing the user to log-in multiple times within a single host session would appear to teach away from the basic inventive principle of the Kung system.

Therefore, for the reasons set forth above, neither Kung nor IEEE Supercomputing, taken alone or in combination, teach or suggest displaying a request for re-authentication at the direction of a system administrator or security officer, or a remote control module or remote control code segment for displaying a request for re-authentication at the direction of a system administrator or security officer. Therefore, the cited art does not teach or suggest all of the claim limitations. Accordingly, the rejection of claims 9, 27 and 38 should be reversed.

CLAIMS 14, 29 AND 40

Claim 14 recites attaching the master password file to a message, encrypting the message with a private key and pass phrase available only to the systems administrator or security officer, and transmitting the message to the plurality of computers. Claim 29 recites a password management module that attaches a master password file containing complete user identifications, associated one-way encrypted passwords and associated privileges to a message, encrypts the message using a private key and pass phrase for the system administrator or security officer and broadcasts the message to all users. Claim 40 recites a password management code segment that attaches a master password file containing a complete user identifications, associated one-way encrypted passwords and associated privileges to a message, encrypts the message using a private key and passphrase for the system administrator or security officer and broadcasts the message to all users.

By contrast, neither of the cited references teach or suggest attaching the master password file to a message, encrypting the message with a private key and pass phrase available only to the systems administrator or security officer, and transmitting the message to the plurality of computers. The Office Action cites Kung in rejecting these claims. However, Kung does not teach updating the password files on the individual computers. The first embodiment of the Kung device has a master password file that each computer uses for authentication (col. 2, lines 16-18). In this embodiment, there is no individual password file on each computer to be updated. In the second embodiment, the master password file is replaced by individual password files on each computer (col. 2, lines 53-55). In the second embodiment, there is no master password file from which to update, nor is there any teaching or suggestion to attach the master password file to a message, encrypt the message with a private key and pass phrase available only to the systems administrator or security officer, and transmitting the message to a plurality of computers.

Kung also teaches away from the present invention. Kung teaches either a system with a file stored at a central location such as a fileserver or workstation that includes the user ID and encrypted password for each computer of the system (col. 2, lines 16-18), or a distributed system where IDs and passwords are stored at each computer in the system (col. 2, lines 53-55). Kung teaches that these systems are mutually exclusive as Kung teaches "[t]he system 10a eliminates the multiple logon server 12 of FIG. 1 and incorporates a secure communication path 20a as part of the network 20 that connects a secure user workstation 11 to the remote host computer 13." Therefore, Kung teaches away from the

present invention as Kung teaches that the multiple logon server, which would have the master password file, is eliminated when each computer has a password file.

Therefore, for the reasons set forth above, neither Kung nor IEEE Supercomputing, taken alone or in combination, teach or suggest attaching the master password file to a message, encrypting the message with a private key and pass phrase available only to the systems administrator or security officer, and transmitting the message to the plurality of computers. Therefore, the cited art does not teach or suggest all of the claim limitations. Accordingly, the rejection of claims 14, 29 and 40 should be reversed.

CLAIMS 15, 30 AND 41

Claim 15 recites reporting to the system administrator or security officer a failure to decrypt a message with a password file attached. Claim 30 recites a password management module that reports a failure to decrypt a message with a password file attached to the system administrator or security officer. Claim 41 recites a password management code segment that reports a failure to decrypt a message with a password file attached to the system administrator or security officer.

By contrast, the passage the Examiner cited in rejecting claim 15 (col. 4, line 60 – col. 5, line 18) discusses an authentication method. A user sends a request for services provided by the remote host computer. The method ascertains if a user is connected to a multiple logon server, and if so, a service connect message is sent back to multiple logon procedure at the user's workstation. The workstation then analyzes the authorization information and sends a service connect to the remote host computer, which accepts the request and connects the user's workstation to the remote host computer. When the remote

host computer requests entry of a user ID and password, the multiple logon procedure sends it to the remote host computer. There is no suggestion or teaching of sending a password file or reporting the failure to decrypt a message with a password file attached to the system administrator or security officer.

Furthermore, in rejecting claims 30 and 41 the examiner cites Kung, FIG. 4, col. 5, lines 38-53 and col. 6, lines 18-50. Applicant respectfully disagrees with the Examiner's interpretation of these sections as applied to these claims. The sections of Kung cited by the Examiner are authentication procedures for a user to connect with a workstation and a remote computer, not a procedure for sending a password file or reporting the failure to decrypt a message with a password file attached to the system administrator or security officer.

FIG. 4 of Kung shows a distributed system that has passwords stored at the workstations. FIG. 4 describes how a user workstation employs a secure communication path to authenticate and automatically logon a user to a remote computer. FIG 4 does not teach or suggest reporting to the system administrator or security officer a failure to decrypt a message with a password file attached. Kung at col. 5, lines 38-53, describes FIG. 4. In operation, a user at a workstation enters a user ID code and password in order to log onto the workstation. A password encryption routine is employed to encrypt the password and ID code and compared against passwords and ID codes stored at the workstation. Kung at col. 6, lines 18-50 describes an authentication procedure used in conjunction with FIG. 4. A user initially logs into a workstation by providing a user ID code and a password. If the user ID and password are the same, the user is logged into the workstation. Kung does not

describe what occurs when the user ID and password do not match. After the user is logged in, when the user desires to access information stored on the remote computer, the procedure requests a secure communication path. After the secure communication path has been established, the procedure transmits the identification (ID) code and encrypted password of the user to the authentication procedure in the remote computer. The authentication procedure, in the remote computer allows the user to log on from the remote workstation. The authentication procedure compares the encrypted password for the user with the one stored in the database coupled to the remote computer. If they are the same, the user is permitted to log onto the remote computer.

Therefore, for the reasons set forth above, neither Kung nor IEEE Supercomputing, taken alone or in combination, teach or suggest reporting to the system administrator or security officer a failure to decrypt a message with a password file attached. Therefore, the cited art does not teach or suggest all of the claim limitations. Accordingly, the rejection of claims 15, 30 and 41 should be reversed.

C. CONCLUSION

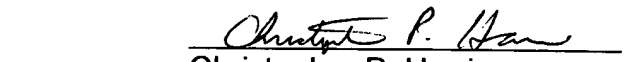
For the reasons set forth above, the rejection of claims 1-41 should be reversed.

9. APPENDIX

Appendix A attached contains a copy of the claims on appeal.

Please charge any deficiency or credit any overpayment in the fees for this Appeal Brief to Deposit Account No. 20-0090.

Respectfully submitted,



Christopher P. Harris
Registration No. 43660

TAROLLI, SUNDHEIM, COVELL,
& TUMMINO L.L.P.
526 Superior Avenue, Suite 1111
Cleveland, Ohio 44114-1400
Phone:(216) 621-2234
Fax: (216) 621-4072

APPENDIX A

1. A method of administering access and security on a network having a plurality of computers, comprising:

installing a one-way encrypted password file on each computer of the plurality of computers in the network, wherein the one-way encrypted password file includes a plurality of user identifications associated one-way encrypted passwords and associated privileges for each authorized user allowed access to the plurality of computers and the network;

one-way encrypting a password entered by a user when the user logs into a computer of the plurality of computers on the network;

checking for a match between the user identification and one-way encrypted password entered by the user and the plurality of user identifications and one-way encrypted passwords stored in the one-way encrypted password file;

enabling access to data and software contained on the computer and the network permitted by the associated privileges for the user when a match is found on the one-way encrypted password file; and

filtering and displaying messages to the user permitted by the associated privileges when a match is found on the one-way encrypted password file.

2. The method recited in claim 1, wherein the associated privileges contained in the one-way encrypted password file indicate the security level and

access privileges of the user identification for access to software, data and messages contained in the computer, the network, and transmitted over the network.

3. The method recited in claim 1, wherein when one or more attempts of the user entering a user identification and one-way encrypted password have failed to match the plurality of user identifications and one-way encrypted passwords contained in the one-way encrypted password file, the method further comprising:

transmitting to a systems administrator or security officer by the computer a notification of the failure to provide a one way encrypted user identification and password that matches a user identification and one-way encrypted password stored on the one-way encrypted password file.

4. The method recited in claim 3, further comprising:

locking, upon request by the systems administrator or security officer, the computer being accessed by the user having at least one failed attempt at entering a user identification and one-way encrypted password so as to permit only access to a login screen by the user.

5. The method recited in claim 3, further comprising:

spoofing, upon request by the systems administrator or security officer, the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user.

6. The method recited in claim 3, further comprising:

disabling, upon request by the systems administrator or security officer, the computer system so that the user cannot access the computer system.

7. The method recited in claim 6, further comprising:

deleting, upon request by the systems administrator or security officer, a plurality of files stored in the computer system.

8. The method recited in claim 1, further comprising:

displaying to a screen on the computer system a request for re-authentication at the direction of a system administrator or security officer.

9. The method recited in claim 8, wherein the request for re-authentication comprises:

displaying a login screen having a position for entry of the user identification and password.

10. The method recited in claim 9, wherein the user identification is a role or title indicative of a level of authority of the user.

11. The method recited in claim 9, further comprising:

accessing a master password file on a computer system accessible by the systems administrator or security officer;

one-way encrypting the password; and

searching the master password file for a match of the user identification and one-way encrypted password.

12. The method recited in claim 11, further comprising:

disabling the computer system, or spoofing the user, or locking the computer system when a match is not found for the user identification and one-way encrypted password in the master password file.

13. The method recited in claim 11, wherein after the user has entered the user identification and one-way encrypted password and the user identification and one-way password has matched that found in the one-way encrypted password file, further comprising:

entering a new password by the user;

re-authenticating the user identification and one-way password stored on the master password file;

one-way encrypting the new password; and

replacing the user identification and password with the one-way encrypted user identification and the new one-way encrypted password in the master password file.

14. The method recited in claim 13, further comprising:

attaching the master password file to a message;

encrypting the message using a private key and pass phrase available only to the systems administrator or security officer; and

transmitting the message to the plurality of computers.

15. The method recited in claim 14, further comprising:

decrypting the message using a public key corresponding to the private key;

reporting to the system administrator or security officer a failure to decrypt the message; and

replacing the one-way encrypted password file with the decrypted master password file.

16. The method recited in claim 1, further comprising:

detecting an anomalous event in a computer of the plurality of computers; and

reporting the anomalous event to a system administrator or security officer.

17. The method recited in claim 16, wherein the anomalous event comprises:

the user has exceeded the number of allowable unsuccessful login attempts;

a change in the users associated privileges has occurred;

a system disable operation was initiated by the user;

a user's password has expired;

a message was rejected due to an invalid digital signature;

a request for remote user re-authentication has been received by the systems administrator or security officer;

a request for a remote user lockout has been received by the system administrator or security officer; and

a request for remote loading passwords has completed successfully on the system administrator or security officer.

18. The method recited in claim 16, further comprising:

deleting a plurality of files on the computer and disabling the computer in response to an anomalous event when requested by the system administrator or security officer or when an immediate shutdown in requested by the user.

19. The method recited in claim 17, further comprising:

disabling the computer system, or spoofing the user, or locking the computer system when an anomalous event occurs.

20. A system to administer access and security on a network having a plurality of computers, comprising:

a one-way encrypted password file on each computer of the plurality of computers in the network, wherein the one-way encrypted password file includes a plurality of user identifications, associated one-way encrypted passwords and associated privileges for each authorized user allowed access to the plurality of computers and the network;

a user login module to receive a user identification or role and password from a user and login the user when a match is found in the one-way encrypted password file; and

a channel monitoring and filtering module to monitor and receive broadcast or multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message.

21. The system recited in claim 20, further comprising:

a password management module to update and insure that all the computers in the network contain the same one-way encrypted password file.

22. The system recited in claim 20, further comprising:

a remote auditing module to monitor and process anomalous events which may

occur on the computer.

23. The system recited in claim 22, wherein the anomalous events comprise:

the user has exceeded the number of allowable unsuccessful login attempts;

a change in the users associated privileges has occurred;

a system disable operation was initiated by the user;

a user's password has expired;

a message was rejected due to an invalid digital signature;

a request for remote user re-authentication has been received by the systems administrator or security officer;

a request for a remote user lockout has been received by the system administrator or security officer; and

a request for remote loading passwords has completed successfully on the system administrator or security officer.

24. The system recited in claim 20, further comprises:

a remote control module to enable a systems administrator or security officer to take appropriate action when an event transpires, wherein the event is an anomalous event.

25. The system recited in claim 24, wherein the appropriate action comprises:

disabling, upon request by the systems administrator or security officer, the computer system so that the user cannot access the computer system; and

deleting, upon request by a systems administrator or security officer, a plurality of files stored in the computer.

26. The system recited in claim 24, wherein the appropriate action comprises:

spoofing, upon request by a systems administrator or security officer, the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user.

27. The system recited in claim 24, wherein the appropriate action comprises:

locking the computer, upon request of a systems administrator or security officer, and displaying a login screen for the user to re-authenticate the user identification and password.

28. The system recited in claim 20, further comprising:

an authentication module to re-authenticate the user after the user login module has found a match in the one-way encrypted password contained in the computer by checking the user identification and password against a master password file stored in a computer accessible by a systems administrator or security officer.

29. The system recited in claim 21, wherein the password management module attaches a master password file containing a complete user identifications, associated one-way encrypted passwords and associated privileges to a message, encrypts the message using a private key and pass phrase for the system administrator or security officer and broadcasts the message to all users.

30. The system recited in claim 29, wherein the password management module decrypts the message using a public key associated with the private key, replaces the one-way encrypted password file when decryption of the message is successful and reports a failure to the system administrator or security officer when the decryption is not successful.

31. A computer program executable by a computer and embedded in a computer readable medium to administer access and security on a network having a plurality of computers, comprising:

a one-way encrypted password file on each computer of the plurality of computers in the network, wherein the one-way encrypted password file includes a plurality of user identifications, associated one-way encrypted passwords and associated privileges for each authorized user allowed access to the plurality of computers and the network;

a user login code segment to receive a user identification or role and password from a user and login the user when a match is found in the one-way encrypted password file; and

a channel monitoring and filtering code segment to monitor and receive broadcast or multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message.

32. The computer program recited in claim 31, further comprising:

a password management code segment to update and insure that all the computers in the network contain the same one-way encrypted password file.

33. The computer program recited in claim 31, further comprising:

a remote auditing code segment to monitor and process anomalous events which may occur on the computer.

34. The computer program recited in claim 33, wherein the anomalous events comprise:

the user has exceeded the number of allowable unsuccessful login attempts;

a change in the users associated privileges has occurred;

a system disable operation was initiated by the user;

a user's password has expired;

a message was rejected due to an invalid digital signature;

a request for remote user re-authentication has been received by the systems administrator or security officer;

a request for a remote user lockout has been received by the system administrator or security officer; and

a request for remote loading passwords has completed successfully on the system administrator or security officer.

35. The computer program recited in claim 31, a remote control code segment to enable a systems administrator or security officer to take appropriate action when an event transpires, wherein the event is an anomalous event.

36. The computer program recited in claim 35, wherein the appropriate action comprises:

disabling, upon request by the systems administrator or security officer, the computer system so that the user cannot access the computer system; and

deleting, upon request by a systems administrator or security officer, a plurality of files stored in the computer.

37. The computer program recited in claim 35, wherein the appropriate action comprises:

spoofing, upon request by a systems administrator or security officer, the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user.

38. The computer program recited in claim 35, wherein the appropriate action comprises:

locking the computer, upon request of a systems administrator or security officer, and displaying a login screen for the user to re-authenticate the user identification and password.

39. The computer program recited in claim 31, further comprising:

an authentication code segment to re-authenticate the user after the user login code segment has found a match in the one-way encrypted password contain in the computer by checking the user identification and password against a master password file stored in a computer accessible by a systems administrator or security officer.

40. The computer program recited in claim 32, wherein the password management code segment attaches a master password file containing a complete user identifications, associated one-way encrypted passwords and associated privileges to a message, encrypts the message using a private key and passphrase for the system administrator or security officer and broadcasts the message to all users.

41. The computer program recited in claim 40, wherein the password management code segment decrypts the message using a public key associated with the private key, replaces the one-way encrypted password file when decryption of the message is successful and reports a failure to the system administrator or security officer when the decryption is not successful.